JOURNAL OF ALGEBRA 158, 1–17 (1993)

Associative Subalgebras of the Griess Algebra

WERNER MEYER AND WOLFRAM NEUTSCH

Max-Planck-Institut für Mathematik,
Gottfried-Claren-Strasse 26, W-5300 Bonn 3, Germany

Communicated by Gernot Stroth

Received September 7, 1990; revised August 29, 1991

The structure of the Griess algebra $\mathfrak{G}$, whose automorphism group is the Fischer–Griess monster F_1, is investigated. We show the existence of 48-dimensional associative subalgebras in $\mathfrak{G}$ and, furthermore, demonstrate that they are not contained in strictly larger ones. This is an immediate consequence of a more general necessary and sufficient criterion for the maximality of associative subalgebras of $\mathfrak{G}$. It is conjectured that the given explicit examples are of maximal possible dimension among all associative subalgebras in $\mathfrak{G}$. This depends on the validity of a certain inequality.

KNOWN RESULTS

In this section we compile a number of known results concerning properties of the Griess algebra. We shall freely use the character tables of the Monster given in Conway *et al.* [3], henceforth referred to as the "ATLAS," although no explicit proofs for their correctness have been published up to now.

Proofs of the other statements described in this section can be found in the literature, especially in Griess [4] and Conway [2]. The largest sporadic group, the Monster F_1, of order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \tag{1}$$

has a minimal representation in characteristic 0 of degree

$$196883 = 47 \cdot 59 \cdot 71 \tag{2}$$

which can be realised over the field $\mathbb{Q}$ of rational numbers [4]. The character table shows that the trivial representation $\underline{1}$ as well as $\underline{196883}$ itself are contained exactly once in the symmetric square $S^2(\underline{196883})$: the precise decomposition is

$$S^2(\underline{196883}) = \underline{1} \oplus \underline{196883} \oplus \underline{842609326} \oplus \underline{18538750076}. \tag{3}$$

0021-8693/93 $5.00

This implies the existence of an F_1-invariant inner product and an F_1-invariant algebra (the "Griess algebra" $\mathfrak{G}$) with unit element 1 on an $\mathbb{R}$-vector space of dimension 196884, on which the Monster acts as

$$\underline{1} \oplus \underline{196883}. \tag{4}$$

Since the above-mentioned characters lie in the symmetric part of the tensor square of $\underline{196883}$, the inner product

$$\langle \cdot, \cdot \rangle : \mathfrak{G} \times \mathfrak{G} \to \mathbb{R} \tag{5}$$

is symmetric and for reasons of irreducibility (without restriction of generality, positive) definite: For all $a, b \in \mathfrak{G}$,

$$\langle a, b \rangle = \langle b, a \rangle \tag{6}$$

and

$$\langle a, a \rangle > 0 \tag{7}$$

if $a \neq 0$.

For the same reason the algebra product, here denoted by a dot or by concatenation of the factors, is commutative:

$$a \cdot b = b \cdot a \tag{8}$$

and, since $\underline{1}$ also is contained exactly once in $\underline{196883}^3$ (namely, in $S^3(\underline{196883})$), the inner product must be associative with respect to the algebra,

$$\langle a \cdot b, c \rangle = \langle a, b \cdot c \rangle. \tag{9}$$

The algebra itself, however, is not associative.

We should note that all these properties can also be deduced immediately from the explicit form of the Griess algebra without invoking the character table.

In the sequel, we shall occasionally use the *(left) multiplication mapping* μ_a for some given element $a \in \mathfrak{G}$, which is defined as

$$\begin{aligned} \mu_a &: \mathfrak{G} \to \mathfrak{G} \\ x &\mapsto \mu_a(x) = a \cdot x. \end{aligned} \tag{10}$$

(Conway denotes this by ad_a.) Because of the associativity of the scalar product, μ_a is a symmetric operator. We use the notation of the ATLAS with the single exception that we choose $\langle \cdot, \cdot \rangle$ as twice the Conway product.

THEOREM 1 [2]. *For two arbitrary vectors a, b the* Norton inequality,

$$\langle a^2, b^2 \rangle \geqslant \langle a \cdot b, a \cdot b \rangle \tag{11}$$

holds.

DEFINITION 1 [2]. Two elements a, b in $\mathfrak{G}$ *associate* if for all $x \in \mathfrak{G}$,

$$a \cdot (x \cdot b) = (a \cdot x) \cdot b. \tag{12}$$

This is clearly tantamount to the commutativity of μ_a and μ_b. One says, *a alternates* with b, if the last equation is fulfilled for $x = a$,

$$a \cdot (a \cdot b) = a^2 \cdot b. \tag{13}$$

Of fundamental importance is the remarkable result which is also ascribed to Norton,

THEOREM 2 [2]. *The following three assertions are equivalent*:

(a) *We have equality in Norton's formula,*

$$\langle a^2, b^2 \rangle = \langle ab, ab \rangle; \tag{14}$$

(b) *a and b associate*;

(c) *a alternates with b (or vice versa).*

DEFINITION 2 [2]. An element which associates with its square is called a *Jordan element*. Trivially, the multiples of idempotents are Jordan.

The connection with the theory of sporadic groups is

THEOREM 3 [2]. *Let*

$$F = \mathrm{Aut}\, \mathfrak{G} \tag{15}$$

be the automorphism group of the Griess algebra. Then the scalar product is invariant under F, because it can be calculated from the algebra product via

$$\mathrm{tr}(\mu_a \mu_b) = 20336 \langle a, 1 \rangle \langle b, 1 \rangle + 4620 \langle a, b \rangle. \tag{16}$$

F is finite; more precisely,

$$F \cong F_1. \tag{17}$$

We associate to each *transposition* ($= 2A$-element in F_1) α the shortest

nonzero idempotent i_α ("transposition idempotent" of α) which lies in the (two-dimensional) fixed point space of

$$C_F(\alpha) \cong 2 \wedge F_2 \tag{18}$$

in $\mathfrak{G}$ such that the *transposition axis* t_α described in Conway [2] is a multiple of i_α,

$$a = t_\alpha = 64 i_\alpha. \tag{19}$$

The axis a fulfills the conditions

$$a \cdot a = 64a \tag{20}$$

and

$$\langle a, a \rangle = 256. \tag{21}$$

We can proceed in the same way for $3A$-elements τ instead of transpositions. This gives idempotents i_τ with norm $\frac{1}{10}$. Conway [2] shows by a simple character-theoretic argument that the normaliser

$$N_F(\alpha) \cong 2 \wedge F_2 \tag{22}$$

of a transposition $\alpha \in 2A$ whose associated idempotent is $i = i_\alpha$ decomposes the Griess algebra into irreducible invariant subspaces contained in the eigenspaces of μ_α as follows:

$$\begin{array}{lcccccc} C(2A) = N(2A) \cong 2 \wedge F_2 \colon & \underline{1} \oplus & \underline{1} \oplus & \underline{4371} \oplus & \underline{96255} \oplus & \underline{96256} & \\ \text{eigenvalues of } \mu_i \colon & 1 \quad 0 & & \tfrac{1}{4} \quad 0 & & \tfrac{1}{32} & \\ \text{eigenvalues of } \alpha \colon & & & +1 & & -1 & \end{array} \tag{23}$$

In precisely the same way, we have the analogous splitting for $\tau \in 3A$:

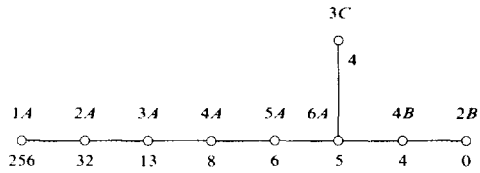
$$\begin{array}{lcccccc} N(3A) \cong 3 \wedge F_{24} \colon & \underline{1} \oplus & \underline{1} \oplus & \underline{8671} \oplus & \underline{57477} \oplus & \underline{1566} \oplus & \underline{129168} \\ \text{eigenvalues of } \mu_i \colon & 1 \quad 0 & & \tfrac{1}{5} \quad 0 & & \tfrac{1}{3} \quad \tfrac{1}{30} & \\ & & & \mathrm{Fix}(\tau) & & \mathrm{Fix}(\tau)^\perp & \end{array} \tag{24}$$

Note that in both cases the eigenvalue 1 occurs just once.

We also mention the important fact ([2], for a proof see Norton [6] and Griess *et al.* [5]) that F acts by conjugation as a rank-9-permutation group on the transpositions and that the product of two transpositions is contained in one of the F_1-classes

$$1A,\ 2A,\ 2B,\ 3A,\ 3C,\ 4A,\ 4B,\ 5A,\ 6A. \tag{25}$$

By an observation of McKay, these classes can be associated in a natural way with the nodes of the extended E_8 Dynkin diagram [2]:



(26)

The numbers attached to the nodes are the inner products of t_α and t_β, where α and β are transpositions whose product is in the appropriate class of F_1.

Associative Subalgebras

The main obstacle for the study of the interior structure of $\mathfrak{G}$ is—besides the large dimension—its non-associativity. It is therefore natural to consider associative subalgebras. Obviously all vectors in such a subalgebra are power-associative, or, what amounts to the same, Jordan elements. In order to investigate the structure of associative subalgebras of $\mathfrak{G}$ we need the easy

Lemma 1. (a) *The only nilpotent Jordan element in* $\mathfrak{G}$ *is* 0;

(b) *There is no subalgebra in* $\mathfrak{G}$ *isomorphic to* $\mathbb{C}$;

(c) *The scalar product of two idempotents is never negative;*

(d) *Two idempotent elements a and b annihilate each other if and only if they are perpendicular.*

(e) *If* $i \in \mathfrak{G}$ *is idempotent,*

$$i^2 = i \tag{27}$$

the norm $\langle i, i \rangle$ *of i lies between 0 and 3 (incl.). The extremal values occur only for* $i \in \{0, 1\}$.

(f) *For all* $a, b \in \mathfrak{G}$,

$$\langle a, b \rangle^2 \leqslant \langle a, a \rangle \langle b, b \rangle \tag{28}$$

(*Schwarz' inequality*).

Proof. (a) If $x \in \mathfrak{G}^\# = \mathfrak{G} \setminus \{0\}$ is nilpotent, there exists a number $k > 0$ such that $x^k \neq 0$ and $x^{k+1} = x^{k+2} = \cdots = 0$. This gives

$$\langle x^k, x^k \rangle = \langle x^k, x^k \cdot 1 \rangle = \langle x^{2k}, 1 \rangle = \langle 0, 1 \rangle = 0. \tag{29}$$

Hence

$$x^k = 0 \tag{30}$$

which contradicts the assumption.

(b) A subalgebra isomorphic to $\mathbb{C}$ would be generated by nonzero vectors e and i, obeying the conditions

$$e \cdot e = e; \qquad e \cdot i = i \cdot e = i; \qquad i \cdot i = -e. \tag{31}$$

But then we would have

$$\langle i, i \rangle = \langle i, i \cdot e \rangle = \langle i^2, e \rangle = \langle -e, e \rangle = -\langle e, e \rangle < 0 \tag{32}$$

which is clearly impossible.

(c) Norton's inequality provides us with

$$\langle a, b \rangle = \langle a^2, b^2 \rangle \geqslant \langle ab, ab \rangle \geqslant 0 \tag{33}$$

for any two idempotent elements a and b.

(d) From

$$a^2 = a; \qquad b^2 = b \tag{34}$$

and

$$a \cdot b = 0 \tag{35}$$

it follows that

$$\langle a, b \rangle = \langle a \cdot a, b \rangle = \langle a, a \cdot b \rangle = 0. \tag{36}$$

The orthogonality of a and b implies

$$0 = \langle a, b \rangle = \langle a^2, b^2 \rangle \geqslant \langle ab, ab \rangle \tag{37}$$

by Norton's inequality, whence the proposition.

(e) is trivial if $i \in \{0, 1\}$. Otherwise, the subalgebra generated by 1 and i is associative and two-dimensional. Its nontrivial idempotents are i and $1 - i$. In fact,

$$\langle i, 1 - i \rangle = 0 \tag{38}$$

and

$$3 = \langle 1, 1 \rangle = \langle i, i \rangle + \langle 1 - i, 1 - i \rangle \tag{39}$$

which implies the assertion.

(f) is a well-known general property of positive definite scalar products.

The above lemma immediately provides us with the structure of associative subalgebras:

THEOREM 4 (Structure theorem). *Let* $\mathfrak{U}$ *be a k-dimensional associative subalgebra of the Griess algebra* $\mathfrak{G}$. *Then*

(a) $\mathfrak{U}$ *is isomorphic to the direct sum of k copies of* $\mathbb{R}$:

$$\mathfrak{U} \cong \mathbb{R}^k \tag{40}$$

(b) $\mathfrak{U}$ *contains a basis of k mutually annihilating idempotent elements which are orthogonal to each other*:

$$a_i \cdot a_j = 0 \tag{41}$$

and

$$\langle a_i, a_j \rangle = 0 \tag{42}$$

for all $i, j \in \{1, ..., k\}$ *with* $i \neq j$.

(c) *The idempotent elements in* $\mathfrak{U}$ *are the partial sums of the* a_i (*and vice versa*). *In particular, there are exactly* 2^k *idempotents in* $\mathfrak{U}$, *including the zero element* 0;

$$\{a_1, ..., a_k\} \tag{43}$$

is the only orthogonal basis among them. We shall call the a_i *the* basic (*or* fundamental) idempotents *of* $\mathfrak{U}$.

Proof. As an associative algebra, $\mathfrak{U}$ contains only Jordan elements. By part (a) of Lemma 1, the Jacobson radical of $\mathfrak{U}$ is therefore zero. Hence $\mathfrak{U}$ is semisimple and thus a direct sum of fields of finite dimension over $\mathbb{R}$, i.e., of algebras isomorphic with $\mathbb{R}$ or $\mathbb{C}$. But $\mathbb{C}$ cannot occur by part b of Lemma 1. This proves (a), while (b) is just the same, except for the orthogonality of the basic idempotents. The latter proposition, however, is a consequence of Lemma 1, part d. (c) follows trivially from the structure of $\mathbb{R}^k$.

All associative subalgebras of $\mathfrak{G}$ are thus generated by systems of mutually perpendicular idempotent elements. It is therefore of great interest to investigate the properties of idempotents in $\mathfrak{G}$. But first we shall give an example.

THEOREM 5. *Let α and β be two different transpositions and*

$$a = i_\alpha \tag{44}$$

and

$$b = i_\beta \tag{45}$$

are the associated idempotents. Then the following statements are equivalent:

(a) *In the Norton formula for a and b, equality holds,*

$$\langle a^2, b^2 \rangle = \langle ab, ab \rangle \tag{46}$$

(b) *a and b associate with each other and for all $x \in \mathfrak{G}$,*

$$a \cdot (x \cdot b) = (a \cdot x) \cdot b \tag{47}$$

(c) *a alternates with b,*

$$a \cdot (a \cdot b) = a^2 \cdot b \tag{48}$$

(d) *b alternates with a,*

$$a \cdot b^2 = (a \cdot b) \cdot b \tag{49}$$

(e) *a and b annihilate each other,*

$$a \cdot b = 0 \tag{50}$$

(f) *a and b are orthogonal,*

$$\langle a, b \rangle = 0 \tag{51}$$

(g) *The product $\alpha\beta$ is a central F_1-involution,*

$$\alpha\beta \in 2B. \tag{52}$$

Proof. The first four properties are tantamount by Theorem 2, as well as the remaining three by Conway [2]. The equivalence of (f) and (g) follows from the scalar product table of the transposition axes which is contained implicitly in the McKay diagram (26).

From the eigenvalue relation

$$a \cdot (a \cdot b) = a^2 \cdot b = a \cdot b \tag{53}$$

we deduce that $a \cdot b$ is linearly depedent of a and similarly (with the rôles of a and b interchanged) of b. This is only possible if

$$a \cdot b = 0 \tag{54}$$

This is (e). The reverse inclusion (e) $\Rightarrow$ (c) is trivial.

A simple consequence is

COROLLARY 1. *Let $\alpha_1, ..., \alpha_k \in 2A$ be pairwise different transpositions and $a_1, ..., a_k$ the corresponding transposition idempotents. The subalgebra $\mathfrak{U}$ of $\mathfrak{G}$ which is generated by $a_1, ..., a_k$ is associative if and only if for all $i, j \in \{1, ..., k\}$ with $i \neq j$,*

$$\alpha_i \alpha_j \in 2B \tag{55}$$

is true. In this case

$$\{4a_1, ..., 4a_k\} \tag{56}$$

is an orthonormal basis of $\mathfrak{U}$; in particular,

$$\dim \mathfrak{U} = k. \tag{57}$$

Furthermore,

$$E = \langle \alpha_1, ..., \alpha_k \rangle \tag{58}$$

is an elementary abelian 2-subgroup of F_1.

Proof. Trivial.

We can now give an upper bound for the dimensions of associative subalgebras of $\mathfrak{G}$ which are generated by transposition axes:

THEOREM 6. (a) *For any associative $\mathfrak{G}$-subalgebra $\mathfrak{U}$, which is generated by transposition idempotents,*

$$\dim \mathfrak{U} \leqslant 48 \tag{59}$$

(b) *Every system of 49 commuting transpositions in F_1 contains at least two whose product is in the class $2A$.*

Proof. Part (b) immediately follows from (a), Corollary 1, and the fact that all F_1-involutions lie in either $2A$ or $2B$. To verify the first statement, we again denote the transposition idempotent by $a_1, ..., a_k$, where

$$k = \dim \mathfrak{U}. \tag{60}$$

By Theorem 3,

$$\{a_1, ..., a_k\} \tag{61}$$

are the basic idempotents, and all of them have the norm

$$\frac{256}{64^2} = \frac{1}{16}. \tag{62}$$

The Structure Theorem shows that they are mutually orthogonal and their sum is an idempotent I of norm

$$\langle I, I \rangle = k/16. \tag{63}$$

Lemma 1.e now gives

$$\langle I, I \rangle \leqslant \langle 1, 1 \rangle = 3 \tag{64}$$

according to our choice of the inner product. A comparison of the last two formulas immediately leads to

$$k \leqslant 48 \tag{65}$$

as required.

We note that the extremal possibility (dimension = 48) can only arise if $1 \in \mathfrak{U}$. The given bound is sharp:

THEOREM 7. *There are* 48 *transpositions in* F_1 *whose pairwise products are in* $2B$.

Proof. In the subgroup

$$O_2(C_F(2B)) \cong 2_+^{1+24} \tag{66}$$

the central factor corresponds to the quotient of the Leech lattice Λ by its double (2Λ). On it, the group

$$C_F(2B)/O_2(2B)) \cong Co_1 \tag{67}$$

acts in a natural way.

The $\Lambda/2\Lambda$-classes may be described by giving the type (Conway [1]) of shortest vectors that they contain. Classes of type 2 are associated with two transpositions each; those of type 3 with two elements of order 4, and those of type 4 with pairs of involutions in $2B$. Thus it suffices to choose 24 vectors $v_1, ..., v_{24}$ in Λ (mod 2Λ) such that the sum of any two of them is of type 4. This is tantamount to the orthogonality (in Λ) of the v_i.

It is easy to find such a set of vectors, for instance,

$$(4, 4, 0^{22}),\ (4, -4, 0^{22}); \qquad (0^2, 4, 4, 0^{20}),\ (0^2, 4, -4, 0^{20}); \quad \ldots \tag{68}$$

in the notation of the ATLAS. The corresponding transposition vectors indeed have 1 as their sum.

The same argument also shows that associative $\mathfrak{G}$-subalgebras of higher dimensions than 48 can only exist if there are nonvanishing idempotents with norm smaller than $\frac{3}{48} = \frac{1}{16}$. We do not know whether this is the case.

It is thus natural to seek the shortest idempotents $\neq 0$ in $\mathfrak{G}$. This is related to determining the maxima of the function

$$F: \mathfrak{G}^{\#} = \mathfrak{G} \setminus \{0\} \to \mathbb{R} \tag{69}$$

defined by

$$F(x) = \frac{\langle x^2, x^2 \rangle}{\langle x, x \rangle^2}. \tag{70}$$

This formulation of the problem allows us to apply the methods of calculus. We first have:

LEMMA 2. *The points a at which F is stationary are characterized by the condition*

$$a^3 \in \mathbb{R}a. \tag{71}$$

Proof. We have to show that for all $\varepsilon \perp a$ the ε-linear terms in $\langle (a+\varepsilon)^2, (a+\varepsilon)^2 \rangle$ vanish. By polarisation we obtain

$$0 = \langle 2a\varepsilon, a^2 \rangle + \langle a^2, 2a\varepsilon \rangle = 4\langle a^2, a\varepsilon \rangle = 4\langle a^3, \varepsilon \rangle, \tag{72}$$

that is, $\varepsilon \perp a^3$. This implies the assertion of the theorem.

It is easy to determine the global minima of F:

THEOREM 8. *The minimal value of F is $\frac{1}{3}$ and is attained at all $a \in \mathfrak{G}$ with*

$$a^2 \in \mathbb{R} \cdot 1 \tag{73}$$

and nowhere else.

Proof. The Schwarz inequality leads with $a = 1$ and $b = x^2$ *to*

$$\langle 1, x^2 \rangle^2 \leqslant \langle 1, 1 \rangle \langle x^2, x^2 \rangle \tag{74}$$

or

$$\langle x, x\rangle^2 \leqslant 3\langle x^2, x^2\rangle; \tag{75}$$

hence

$$F(x) \geqslant \tfrac{1}{3}. \tag{76}$$

Equality holds if and only if x^2 is linearly dependent on 1.

The calculation of the global maxima of F seems to be considerably more difficult, and we have not yet succeeded to determine them. The stationarity condition of Lemma 2 for F is fulfilled for every idempotent element a. In that case, $F(a)$ is simply reciprocal to $\langle a, a\rangle$. Choosing a as a transposition idempotent gives

$$F(a) = 16. \tag{77}$$

To determine the character of the function in the vicinity of a, we have to develop $F(a+\varepsilon) - F(a)$ up to second order in ε. Since μ_a is a symmetric operator, we may find a basis of $a^\perp$ which consists of eigenvectors of μ_a.

Thus we assume $\varepsilon \perp a$ and

$$a \cdot \varepsilon = \mu_a(\varepsilon) = \alpha\varepsilon \tag{78}$$

with $\alpha \in \mathbb{R}$. To the required degree of approximation,

$$\langle a+\varepsilon, a+\varepsilon\rangle = \langle a, a\rangle + \langle \varepsilon, \varepsilon\rangle = \tfrac{1}{16}\,[1 + 16\langle \varepsilon, \varepsilon\rangle] \tag{79}$$

and, therefore,

$$\langle a+\varepsilon, a+\varepsilon\rangle^{-2} \approx 16^2[1 - 32\langle \varepsilon, \varepsilon\rangle]. \tag{80}$$

Furthermore,

$$\langle (a+\varepsilon)^2, (a+\varepsilon)^2\rangle = \langle a^2 + 2\alpha\varepsilon + \varepsilon^2, a^2 + 2\alpha\varepsilon + \varepsilon^2\rangle \tag{81}$$

from which we deduce the relation

$$\langle (a+\varepsilon)^2, (a+\varepsilon)^2\rangle \approx \tfrac{1}{16} + (2\alpha + 4\alpha)\langle \varepsilon, \varepsilon\rangle. \tag{82}$$

Multiplying both approximations, we obtain

$$\begin{aligned} F(a+\varepsilon) - F(a) \approx & -16 + 16^2[1 - 32\langle \varepsilon \cdot \varepsilon\rangle] \\ & \times [\tfrac{1}{16} + (2\alpha + 4\alpha^2)\langle \varepsilon, \varepsilon\rangle] \end{aligned} \tag{83}$$

or, simpler,

$$F(a+\varepsilon) - F(a) \approx -512\langle \varepsilon, \varepsilon\rangle(1 - \alpha - 2\alpha^2). \tag{84}$$

By Conway [2], the eigenvalues of μ_a on $a^\perp$ are $\frac{1}{4}$, $\frac{1}{32}$, and 0; thus the quadratic form in ε given by the last formula is negative definite there. We have proved

THEOREM 9. *Let a be a transposition vector in $\mathfrak{G}$. Then F has a local maximum at a with $F(a) = 16$.*

Next we want to give a characterisation of the maximal associative subalgebras of $\mathfrak{G}$ (i.e., those which are not contained in a strictly larger one). We begin with

DEFINITION 3. An idempotent $a \in \mathfrak{G}$ is *decomposable* if it can be expressed as a sum of at least two nonzero idempotents.

This is a well-known concept, and we deduce

THEOREM 10. *Let*

$$a = \sum_{i=1}^{k} e_i \tag{85}$$

with idempotents a; $e_1, \ldots, e_k$. Then

(a) *the e_i are mutually orthogonal;*

(b) *for all $i \neq j$, e_i and e_j annihilate each other; and*

(c) *the algebra generated by the e's is associative.*

Proof. (b) and (c) immediately follow from (a). Thus it will be sufficient to prove the orthogonality. Application of Norton's inequality and the associativity of the scalar product leads to

$$\sum_i \langle e_i, e_i \rangle = \sum_i \langle 1, e_i^2 \rangle = \sum_i \langle 1, e_i \rangle = \langle 1, a \rangle = \langle 1, a^2 \rangle = \langle a, a \rangle$$

$$= \sum_{i,j} \langle e_i, e_j \rangle = \sum_i \langle e_i, e_i \rangle + \sum_{i \neq j} \langle e_i, e_j \rangle$$

and thus

$$\sum_{i \neq j} \langle e_i, e_j \rangle = 0. \tag{87}$$

In this sum, all terms are $\geqslant 0$ by part (c) of Lemma 1, so all vanish individually, and the theorem is proved.

We are now prepared to characterise the indecomposable idempotents:

THEOREM 11. *An idempotent $a \in \mathfrak{G}$ is indecomposable if and only if the fixed space of μ_a is at most one-dimensional.*

Proof. Set

$$\mathfrak{B} = \mathrm{Fix}(\mu_a) = \{x \in \mathfrak{G} \mid \mu_a(x) = a \cdot x = x\}. \tag{88}$$

For all $x, y \in \mathfrak{B}$, we have

$$a \cdot (ay) = a \cdot y = a^2 \cdot y; \tag{89}$$

hence y associates with a, and consequently

$$\mu_a(xy) = a \cdot (xy) = (ax) \cdot y = xy \tag{90}$$

and $xy \in \mathfrak{B}$. In other words: $\mathfrak{B}$ is an algebra.

Now suppose a is decomposable. Then it has a representation of the form

$$a = \sum_{i=1}^{k} e_i \tag{91}$$

with $e_i^2 = e_i \neq 0$ and $k \geqslant 2$.

By the last theorem, the e_i span a vector space of dimension k, and moreover, for $1 \leqslant j \leqslant k$, we have

$$\mu_a(e_j) = a \cdot e_j = \sum_{i=1}^{k} e_i \cdot e_j = e_j^2 = e_j \tag{92}$$

or $e_j \in \mathfrak{B}$. This implies

$$\dim \mathfrak{B} \geqslant k \geqslant 2. \tag{93}$$

Now assume $\dim \mathfrak{B} \geqslant 2$ and consider the function

$$\varphi: \mathfrak{B}^{\#} = \mathfrak{B} \setminus \{0\} \to \mathbb{R} \tag{94}$$

which is defined by

$$\varphi(x) = \frac{\langle x, x^2 \rangle}{\langle x, x \rangle^{3/2}}; \tag{95}$$

φ is very similar to the function F discussed in detail above. A brief calculation shows that x is a stationary point of φ precisely when, for all $\varepsilon \in \mathfrak{B}$, $\varepsilon \perp x$,

$$\langle x, \varepsilon^2 \rangle = 0 \tag{96}$$

holds. Since $\mathfrak{B}$ is an algebra and $x \in \mathfrak{B}$, we find that this implies

$$x^2 = \lambda x \tag{97}$$

for suitable $\lambda \in \mathbb{R} \setminus \{0\}$. The stationary points of φ therefore are just the real multiples of the idempotents in $\mathfrak{B}$.

If φ is not constant, it attains a maximum and a minimum in $\mathfrak{B}^*$. This provides us with two linearly independent idempotents in $\mathfrak{B}$. The same conclusion can be drawn, however, if φ is constant, for then all x in $\mathfrak{B}^*$ are stationary points and thus multiples of idempotents (note that $\dim \mathfrak{B} \geqslant 2$!). In any case, we can find at least one $b \in \mathfrak{B} \setminus \{0, a\}$. But then $a - b$ is idempotent as well,

$$(a-b)^2 = a^2 + b^2 - 2ab = a + b - 2b = a - b, \tag{98}$$

and we have the nontrivial decomposition

$$a = b + (a - b) \tag{99}$$

which proves the theorem.

The remark in the foregoing section concerning the eigenspaces of elements in the F_1-classes $2A$ and $3A$ at once leads to

COROLLARY 2. *Transposition idempotents and $3A$-idempotents are indecomposable.*

The last result allows us to derive a useful criterion for the maximality of associative $\mathfrak{G}$-subalgebras:

THEOREM 12. *Let $\mathfrak{U}$ be an associative subalgebra of the Griess algebra. Then $\mathfrak{U}$ is maximal associative if and only if the following two conditions are fulfilled*:

(1) *The unit element* 1 *of* $\mathfrak{G}$ *lies in* $\mathfrak{U}$;

(2) *the fundamental idempotents of* $\mathfrak{U}$ *are indecomposable.*

Proof. Set

$$k = \dim \mathfrak{U} \tag{100}$$

and denote the basic idempotents in $\mathfrak{U}$ by

$$\{a_1, \ldots, a_k\}. \tag{101}$$

First assume that $\mathfrak{U}$ has both properties described in the theorem and that $\mathfrak{B}$ is an associative algebra containing $\mathfrak{U}$, whose basic idempotents are

$$\{b_1, ..., b_n\} \tag{102}$$

with

$$n = \dim \mathfrak{B} \geqslant \dim \mathfrak{U} = k. \tag{103}$$

Then all a_i ($i \in \{1, ..., k\}$) are idempotent elements in $\mathfrak{B}$, so by the Structure Theorem they can be written as partial sums of the b_j. Since a_i is indecomposable by assumption, however, this sum cannot contain more than one term. Thus $\{a_i\}$ is a subset of $\{b_j\}$.

But—again by the Structure Theorem—the sum of the norms of all fundamental idempotents in either of $\mathfrak{U}$ and $\mathfrak{B}$ equals the norm of the longest idempotent in the algebra which is 1 in both cases. This gives

$$\sum_{i=1}^{k} \langle a_i, a_i \rangle = \sum_{j=1}^{n} \langle b_j, b_j \rangle = \langle 1, 1 \rangle = 3 \tag{104}$$

and, clearly,

$$\{a_1, ..., a_k\} = \{b_1, ..., b_n\}. \tag{105}$$

Therefore $\mathfrak{U}$ and $\mathfrak{B}$ coincide. Hence $\mathfrak{U}$ is maximal associative.

If, on the other hand, there is no associative algebra containing $\mathfrak{U}$ strictly, obviously $1 \in \mathfrak{U}$, for otherwise we could enlarge $\mathfrak{U}$ by adjoining 1.

So it only remains to show that the a_i are indecomposable. If not, one of them, for instance a_1, could be replaced by a sum of the form

$$a_1 = \sum_{m=1}^{p} e_m \tag{106}$$

with

$$e_m^2 = e_m \neq 0 \tag{107}$$

and $p \geqslant 2$. By Theorem 10,

$$\langle e_1, e_m \rangle = 0 \tag{108}$$

for $1 \neq m$, and, furthermore, for all j, $2 \leqslant k$, we obtain

$$\sum_{m=1}^{p} \langle e_m, a_j \rangle = \langle a_1, a_j \rangle = 0. \tag{109}$$

By Lemma 1, part c, this implies that

$$\{e_1, ..., e_p; a_2, ..., a_k\} \tag{110}$$

is a set of pairwise orthogonal idempotents which generate an associative algebra $\mathfrak{B}$, say. But $\mathfrak{B}$ contains all generators of $\mathfrak{U}$ and has dimension

$$\dim \mathfrak{B} = p + k - 1 \geqslant k + 1. \tag{111}$$

This leads to $\mathfrak{U} < \mathfrak{B}$, in contradiction to the maximality of $\mathfrak{U}$, and the theorem is proved.

An immediate consequence is

COROLLARY 3. *Those* 48*-dimensional associative* $\mathfrak{G}$*-subalgebras, which are generated by transposition axes, are maximal associative.*

ACKNOWLEDGMENT

We thank the unknown referee for a number of suggestions which led to an improvement of the manuscript.

REFERENCES

1. J. H. CONWAY, Three lectures on exceptional groups, *in* "Finite Simple Groups" (M. B. Powell and G. Higman Eds.), Academic Press, London/New York, 1971.
2. J. H. CONWAY, A simple construction for the Fischer–Griess monster group, *Invent. Math.* **79** (1984), 513–540.
3. J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER, AND R. A. WILSON, "ATLAS of Finite Groups," Clarendon Press, Oxford, 1985.
4. R. L. GRIESS, The friendly giant, *Invent. Math.* **69** (1982), 1–102.
5. R. L. GRIESS, U. MEYERFRANKENFELD, AND Y. SEGEV, A uniqueness proof for the monster, *Ann. Math.* **130** (1989), 567–602.
6. S. P. NORTON, The uniqueness of the monster, *in* "Finite Groups Coming of Age" (J. McKay, Ed.), Contemp. Math., Vol. 45, pp. 271–285, Amer. Math. Soc., Providence, RI, 1982.